ON THE CONSTRUCTION OF FINITE OSCILLATOR DICTIONARY

RONGQUAN FENG, ZHENHUA GU, ZILONG WANG, HONGFENG WU, AND KAI ZHOU

Abstract. A finite oscillator dictionary which has important applications in sequences designs and the compressive sensing was introduced by Gurevich, Hadani and Sochen. In this paper, we first revisit closed formulae of the finite split oscillator dictionary $\mathfrak{S}^s$ by a simple proof. Then we study the non-split tori of the group $SL(2,\mathbb{F}_p)$. Finally, An explicit algorithm for computing the finite non-split oscillator dictionary $\mathfrak{S}^{ns}$ is described.

1. Introduction

Let $\mathbb{F}_p$ ($p>3$) be the finite field with p elements, $\mathcal{H}=\mathbb{C}(\mathbb{F}_p)$ be a Hilbert space containing all the functions from $\mathbb{F}_p$ to $\mathbb{C}$ with Hermitian product

$$\langle f,g\rangle=\sum_{t\in\mathbb{F}_p} f(t)\overline{g(t)},$$

for $f,g\in\mathcal{H}$, and let $U(\mathcal{H})$ be the group of unitary operators on $\mathcal{H}$. Define L_τ, M_ω, and $F\in U(\mathcal{H})$ by

$$L_\tau f(t)=f(t+\tau),$$
$$M_\omega f(t)=e^{\frac{2\pi i}{p}\omega t}f(t),$$

and

$$\hat{f}=F(f)(j)=\frac{1}{\sqrt{p}}\sum_{t\in\mathbb{F}_p} e^{\frac{2\pi i}{p}jt}f(t),$$

for $\tau,\ \omega\in\mathbb{F}_p$ and $f\in\mathcal{H}$. These operators L_τ, M_ω and F are called the time shift, the phase shift and the Fourier transform respectively which are important operators in signal processings.

Denote by $SL(2,\mathbb{F}_p)$ the special linear group of 2×2 nonsingular matrices over $\mathbb{F}_p$ with determinant one. By studying the Weil representation $\rho: SL(2,\mathbb{F}_p)\to U(\mathcal{H})$, a finite oscillator dictionary $\mathfrak{S}$ was given in [3] which has the following properties:

(i) Autocorrelation (ambiguity function). For every $\varphi\in\mathfrak{S}$,

$$|\langle\varphi,M_\omega L_\tau\varphi\rangle|=\begin{cases}1, & \text{if } \tau=\omega=0;\\ \le\frac{2}{\sqrt{p}}, & \text{otherwise.}\end{cases}$$

(ii) Cross correlation (cross ambiguity function). For every $\phi,\varphi\in\mathfrak{S}$, $\phi\ne\varphi$,

$$|\langle\phi,M_\omega L_\tau\varphi\rangle|\le\frac{4}{\sqrt{p}},\qquad \text{for every } \tau,\omega\in\mathbb{F}_p.$$

2000 *Mathematics Subject Classification.* 11F27, 94A12.

Key words and phrases. Weil representation, finite harmonic oscillator, torus, DFT.

The first author was supported by NSF of China (No. 10990011). The fourth author is supported by China Postdoctoral Science Foundation funded project.

(iii) Supremum. For every $\varphi \in \mathfrak{S}$,

$$\max\{|\varphi(t)| : t \in \mathbb{F}_p\} \leq \frac{2}{\sqrt{p}}.$$

(iv) Fourier invariance. For every $\varphi \in \mathfrak{S}$, its Fourier transform $\hat{\varphi}$ is (up to multiplication by a unitary scalar) also in $\mathfrak{S}$.

The properties above make the finite oscillator dictionary $\mathfrak{S}$ ideal for some applications. Please refer to [3, 12] for the application in the discrete radar and communication systems [2], and refer to [4, 7] for the application in the emerging fields of sparsity and the compressive sensing. Besides, the Weil representation on $SL(2, \mathbb{F}_p)$ provides a new approach for the diagonalization of the discrete Fourier transform [5, 13], and a proof for quadratic reciprocity [6]. Therefore, vectors in $\mathfrak{S}$ should be given in closed form or by an algorithm. In fact, $\mathfrak{S}$ can be divided into two parts naturally, split case $\mathfrak{S}^s$ and non-split case $\mathfrak{S}^{ns}$. The split case $\mathfrak{S}^s$ was given by an algorithm in [3], and then closed formulae was given in [12]. In this paper, by studying the tori of $SL(2, \mathbb{F}_p)$, closed formulae of the split case $\mathfrak{S}^s$ were revisited by a simple proof, and an explicit algorithm for constructing the non-split case $\mathfrak{S}^{ns}$ is described.

The rest of the paper is organized as follows. The oscillator system constructed in [3] is described in Section 2. Closed formulae of the split case of the finite oscillator dictionary $\mathfrak{S}^s$ are revisited in Section 3. In Section 4, based on the stucture of the non-split tori of the group $SL(2, \mathbb{F}_p)$, an explicit algorithm for computing the non-split case of the finite oscillator dictionary $\mathfrak{S}^{ns}$ is described.

2. Finite Oscillator Dictionary

In this section, the finite oscillator dictionary proposed by Gurevich, Hadani and Sochen in [3, 4] was introduced. For more details about the representation theory and the Weil representation, we refer the reader to [10, 11, 14, 15].

Since $SL(2, \mathbb{F}_p)$ is generated by $g_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, $g_b = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$, and the Weyl element $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, where $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$, the Weil representation ρ can be determined by $\rho(g_a), \rho(g_b)$ and $\rho(w)$ which are given as follows.

$$\rho(g_a)(f)(t) = \sigma(a) f(a^{-1}t), \tag{2.1}$$

$$\rho(g_b)(f)(t) = \chi(-2^{-1}bt^2) f(t), \tag{2.2}$$

$$\rho(w)(f)(j) = \frac{1}{\sqrt{p}} \sum_{t \in \mathbb{F}_p} \chi(tj) f(t), \tag{2.3}$$

where χ is an additive character of $\mathbb{F}_p$ with $\chi(a) = e^{\frac{2\pi i}{p} a}$, and σ is the Legendre character, i.e., $\sigma(a) = (\frac{a}{p})$. Here $\rho(w) = F$ is the discrete Fourier transform. Denote by S_a the operator $\rho(g_a)$, and by N_b the operator $\rho(g_b)$ for convenience. For any $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_p)$, if $b \neq 0$,

$$g = \begin{pmatrix} a & b \\ (ad-1)b^{-1} & d \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ bd & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ ab^{-1} & 1 \end{pmatrix}.$$

Then the Weil representation of g is given by

$$\rho(g) = S_b \circ N_{bd} \circ F \circ N_{ab^{-1}}. \tag{2.4}$$

If $b = 0$, then

$$g = \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ ac & 1 \end{pmatrix}.$$

Hence the Weil representation of g can be described as

$$\rho(g) = S_a \circ N_{ac}. \tag{2.5}$$

A maximal *algebraic torus* in $SL(2, \mathbb{F}_p)$ is a maximal commutative subgroup which becomes diagonalizable over the original field $\mathbb{F}_p$ or over the quadratic extension of $\mathbb{F}_p$. One standard example of a maximal algebraic torus in $SL_2(\mathbb{F}_p)$ is the standard diagonal torus

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_p^* \right\}.$$

Up to conjugation, there are two classes of maximal algebraic tori in $SL(2, \mathbb{F}_p)$. The first class, called *split tori*, consists of those tori which are diagonalizable over $\mathbb{F}_p$. Every split torus T is conjugated to the standard diagonal torus A, i.e., there exists an element $g \in SL(2, \mathbb{F}_p)$ such that $g \cdot T \cdot g^{-1} = A$. The second class, called *non-split tori*, consists of those tori which are not diagonalizable over $\mathbb{F}_p$, but become diagonalizable over the quadratic extension $\mathbb{F}_{p^2}$ of $\mathbb{F}_p$. In fact, a split torus is a cyclic subgroup of $SL(2, \mathbb{F}_p)$ with order $p-1$, while a non-split torus is a cyclic subgroup of $SL(2, \mathbb{F}_p)$ with order $p + 1$.

All split (non-split) tori are conjugated to one another, so the number of split (non-split) tori equals to the number of elements in the coset space $SL(2, \mathbb{F}_p)/N_A$ ($SL(2, \mathbb{F}_p)/N_T$), where N_A (N_T) is the normalizer group of A (non-split torus T). Thus

$$|(SL_2(\mathbb{F}_p)/N_A)| = \frac{1}{2}p(p+1) \qquad \text{and} \qquad |(SL_2(\mathbb{F}_p)/N_T)| = \frac{1}{2}p(p-1). \tag{2.6}$$

Since every maximal torus $T \in SL(2, \mathbb{F}_p)$ is a cyclic group, we obtain a decomposition of $\rho_{|T} : T \to U(\mathcal{H})$, the restriction of the Weil representation ρ on T, corresponding to an orthogonal decomposition of $\mathcal{H}$ as

$$\rho_{|T} = \bigoplus_{\chi \in \Lambda_T} \chi \quad \text{and} \quad \mathcal{H} = \bigoplus_{\chi \in \Lambda_T} \mathcal{H}_\chi, \tag{2.7}$$

where Λ_T is the collection of all the one dimensional subrepresentation (character) $\chi : T \to \mathbb{C}$ of T.

The decomposition (2.7) depends on the type of T. If T is a split torus, χ is a character given by $\chi : \mathbb{Z}_{p-1} \to \mathbb{C}$. We have $\dim \mathcal{H}_\chi = 1$ if χ is not the Legendre character σ, and $\dim \mathcal{H}_\sigma = 2$. If T is a non-split torus, then χ is a character given by $\chi : \mathbb{Z}_{p+1} \to \mathbb{C}$. We have $\dim \mathcal{H}_\chi = 1$ for every non-quadratic character χ.

For a given torus T, choosing a vector $\varphi_\chi \in \mathcal{H}_\chi$ of unit norm for each character $\chi \in \Lambda_T$, we obtain a collection of orthonormal vectors

$$\mathcal{B}_T = \{\varphi_\chi : \chi \in \Lambda_T, \chi \neq \sigma \text{ if } T \text{ is split}\}. \tag{2.8}$$

Considering the union of all these collections, we obtain the finite oscillator dictionary

$$\mathfrak{S} = \{\varphi \in \mathcal{B}_T : T \text{ is a maximal torus of } SL(2,\mathbb{F}_p)\} = \bigcup_T \mathcal{B}_T, \tag{2.9}$$

where T runs through all maximal tori of $SL(2,\mathbb{F}_p)$.

The finite oscillator dictionary $\mathfrak{S}$ is naturally separated into two sub-dictionaries $\mathfrak{S}^s$ and $\mathfrak{S}^{ns}$ corresponding to the split and non-split tori respectively. That is, $\mathfrak{S}^s$ ($\mathfrak{S}^{ns}$) consists of the union of $\mathcal{B}_T$ where T runs through all the split tori (non-split tori) in $SL(2,\mathbb{F}_p)$. Totally there are $\frac{1}{2}p(p+1)$ $(\frac{1}{2}p(p-1))$ split (non-split) tori which consisting of $p-2$ (p) orthonormal vectors each. Therefore

$$|\mathfrak{S}^s| = \frac{1}{2}p(p+1)(p-2) \quad \text{and} \quad |\mathfrak{S}^{ns}| = \frac{1}{2}p^2(p-1). \tag{2.10}$$

For a given maximal torus T, an efficient way to specify the decomposition (2.7) is by choosing a generator $g_T \in T$, the character is determined by the eigenvalue of the linear operator $\rho(g_T)$, and the character space is corresponding to the eigenspace naturally. Thus we can diagonalize $\rho(g_T)$ and obtain the basis $\mathcal{B}_T$. Let N_T be the normalizer of the group T and R_T be a system of coset representatives of N_T in $SL(2,\mathbb{F}_p)$. Since all the maximal split or non-split tori are conjugated to one another, all the maximal tori which are of the same type with T (split or non-split) can be written as gTg^{-1}, where $g \in R_T$. Since

$$\mathcal{B}_{gTg^{-1}} = \{\rho(g)\varphi :\ \varphi \in \mathcal{B}_T\}, \tag{2.11}$$

the oscillator dictionary $\mathfrak{S}^s$ or $\mathfrak{S}^{ns}$ can be represented by

$$\bigcup_{g\in R_T} \mathcal{B}_{gTg^{-1}} = \{\rho(g)\varphi : g \in R_T, \varphi \in \mathcal{B}_T\}. \tag{2.12}$$

3. The Split Case: $\mathfrak{S}^s$

In this section, we revisit the results in [12] by a simple proof. Based on (2.12),

$$\mathfrak{S}^s = \{\rho(g)\varphi : g \in R_A, \varphi \in \mathcal{B}_A\}, \tag{3.1}$$

we need only to compute $\mathcal{B}_A$ and R_A.

Let α be a generator of $\mathbb{F}_p^*$, define the multiplicative character ψ_j as $\psi_j(\alpha^k) = e^{\frac{2\pi i}{p-1}jk}$ for $k = 0, 1, \cdots, p-2$ and $\psi_j(0) = 0$ for $j \neq 0$ and $\psi_0(0) = 1$. Then $\nabla = \{\psi_0, s\psi_1, \cdots, s\psi_{p-2}\}$, where $s = (p-1)^{-1/2}$, is an orthonormal basis of the Hilbert space $\mathcal{H}$. For $j \neq 0$, by (2.1), we have

$$S_\alpha(s\psi_j)(\alpha^k) = \sigma(\alpha)s\psi_j(\alpha^{-1}\alpha^k) = -s\psi_j(\alpha^{k-1}) = -se^{-\frac{2\pi ij}{p-1}}\psi_j(\alpha^k).$$

Noting that $S_\alpha(s\psi_j)(0) = 0$, we have

$$S_\alpha(s\psi_j) = -e^{-\frac{2\pi ij}{p-1}} \cdot s\psi_j.$$

Thus $s\psi_j$ is an eigenvector of S_α associated with the eigenvalue $-e^{-\frac{2\pi ij}{p-1}} \neq -1$. Therefore,

$$\mathcal{B}_A = \{s\psi_j : 1 \le j \le p-2\}. \tag{3.2}$$

Combining the result in [12] that

$$R_A = \left\{ \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} : 0 \le b \le \frac{p-1}{2}, c \in \mathbb{F}_p \right\}$$

and (3.1), vectors in $\mathfrak{S}^s$ can be described in closed formulae [12] easily as

$$\mathfrak{S}^s = \{\varphi_{x,y,z} : \ 1 \le x \le p-2, 0 \le y \le p-1, 0 \le z \le (p-1)/2\},$$

where

$$\varphi_{x,y,0}(t) = \frac{1}{\sqrt{p-1}} \psi_x(t)\chi(yt^2),$$

and

$$\varphi_{x,y,z}(t) = \frac{\chi(yt^2)}{\sqrt{p(p-1)}} \sum_{j=1}^{p-1} \psi_x(j)\chi(-(2z)^{-1}(j-t)^2) \text{ for } z \neq 0.$$

4. The Non-Split Case: $\mathfrak{S}^{ns}$

In this section we give the details of the construction of $\mathfrak{S}^{ns}$. Let us first consider the structure of a non-split torus.

Lemma 4.1. *Let D be a non-square element of $\mathbb{F}_p$. Then*

$$T_D = \left\{ \begin{pmatrix} x & y \\ Dy & x \end{pmatrix} : x^2 - Dy^2 = 1, x, y \in \mathbb{F}_p \right\}$$

is a maximal non-split torus.

Proof. Let

$$G_D = \left\{ \begin{pmatrix} x & y \\ Dy & x \end{pmatrix} : x^2 - Dy^2 \neq 0, x, y \in \mathbb{F}_p \right\}.$$

It is easy to check that G_D is isomorphic to $\mathbb{F}_{p^2}^*$ by the isomorphism given by

$$\begin{pmatrix} x & y \\ Dy & x \end{pmatrix} \mapsto x + \sqrt{D}y. \tag{4.1}$$

Thus T_D can be diagonalized over $\mathbb{F}_{p^2}$ as a subgroup of G_D. Note that the eigenvalues of $\begin{pmatrix} x & y \\ Dy & x \end{pmatrix} \in T_D$ lie in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Hence T_D is a non-split torus. $\square$

Theorem 4.2. (1) *Let D be a non-square element of $\mathbb{F}_p$ and $s+\sqrt{D}t$ be a primitive element of $\mathbb{F}_{p^2}$, then T_D is a cyclic group of order $p+1$ with a generator*

$$\begin{pmatrix} \frac{s^2+Dt^2}{s^2-Dt^2} & \frac{-2st}{s^2-Dt^2} \\ \frac{-2stD}{s^2-Dt^2} & \frac{s^2+Dt^2}{s^2-Dt^2} \end{pmatrix}.$$

(2) *The normalizer of T_D in $SL(2, \mathbb{F}_p)$ is*

$$N_D = \left\{ \begin{pmatrix} a & b \\ bD & a \end{pmatrix}, \begin{pmatrix} x & y \\ -yD & -x \end{pmatrix} : a^2 - b^2D = y^2D - x^2 = 1, a, b, x, y \in \mathbb{F}_p \right\}.$$

Proof. (1) By the isomorphism (4.1), $\begin{pmatrix} s & t \\ Dt & s \end{pmatrix}$ is a generator of the cyclic group G_D. Since $\frac{|G_D|}{|T_D|} = p-1$, $\begin{pmatrix} s & t \\ Dt & s \end{pmatrix}^{p-1}$ is a generator of the cyclic subgroup T_D. From

$$(s+\sqrt{D}t)^{p-1} = \frac{(s+\sqrt{D}t)^p}{s+\sqrt{D}t} = \frac{s-\sqrt{D}t}{s+\sqrt{D}t} = \frac{s^2+Dt^2-2st\sqrt{D}}{s^2-Dt^2},$$

we know that

$$\begin{pmatrix} s & t \\ Dt & s \end{pmatrix}^{p-1} = \begin{pmatrix} \frac{s^2+Dt^2}{s^2-Dt^2} & \frac{-2st}{s^2-Dt^2} \\ \frac{-2stD}{s^2-Dt^2} & \frac{s^2+Dt^2}{s^2-Dt^2} \end{pmatrix}$$

is a generator of T_D.

(2) Suppose $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N_D$. Then for every $\begin{pmatrix} x & y \\ Dy & x \end{pmatrix} \in T_D$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ Dy & x \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} x+bdyD-acy & a^2y-b^2yD \\ d^2yD-c^2y & x+acy-bdyD \end{pmatrix} \in T_D,$$

which implies

$$\left\{ \begin{array}{rcl} ac-bdD &=& 0, \\ c^2-d^2D &=& b^2D^2-a^2D. \end{array} \right. \tag{4.2}$$

Combining (4.2) with

$$ad-bc=1, \tag{4.3}$$

we have $g = \begin{pmatrix} a & b \\ bD & a \end{pmatrix}$ with $a^2-b^2D=1$ or $g = \begin{pmatrix} a & b \\ -bD & -a \end{pmatrix}$ with $a^2-b^2D = -1$. Therefore,

$$N_D = \left\{ \begin{pmatrix} a & b \\ bD & a \end{pmatrix}, \begin{pmatrix} x & y \\ -yD & -x \end{pmatrix} : a^2-b^2D=1, y^2D-x^2=1, a,b,x,y \in \mathbb{F}_p \right\}.$$

□

Denote by $\pm\sqrt{-1}$ the two roots of the equation $X^2+1=0$. If $p \equiv 3 \pmod 4$, -1 is a non-square element, then $\pm\sqrt{-1} \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. If $p \equiv 1 \pmod 4$, -1 is a square element and $\pm\sqrt{-1} \in \mathbb{F}_p$. Now we define S as a subset of $\mathbb{F}_p$ satisfying (i) for every $x \in S$, $1 \le x \le \frac{p-1}{2}$, and (ii) $x \in S \Leftrightarrow \pm\sqrt{-1}x \notin S$. It is obvious that $|S| = \frac{p-1}{4}$.

Theorem 4.3. (1) *If* $p \equiv 3 \pmod 4$*, let*

$$R_D = \left\{ \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix} : 1 \le a \le \frac{p-1}{2}, 0 \le c \le p-1 \right\},$$

then R_D *is a collection of coset representatives of* N_D *in* $SL(2,\mathbb{F}_p)$.

(2) *If* $p \equiv 1 \pmod 4$*, let*

$$R_D^{'} = \left\{ \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}, \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : a \in S, 0 \le c \le p-1 \right\},$$

then $R_D^{'}$ *is a collection of coset representatives of* N_D *in* $SL(2,\mathbb{F}_p)$.

Proof. (1) For $p \equiv 3 \pmod 4$, suppose that $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{F}_p)$. Since -1 is a non-square element, one of the equations $\xi^2 = \frac{b^2}{b^2D-a^2}$ and $\xi^2 = \frac{b^2}{a^2-b^2D}$ is solvable over $\mathbb{F}_p$ for $b \neq 0$. If y is a root of $\xi^2 = \frac{b^2}{b^2D-a^2}$, let $x = \frac{ay}{b}$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ -Dy & -x \end{pmatrix} = \begin{pmatrix} ax-byD & 0 \\ cx-dyD & cy-dx \end{pmatrix}. \tag{4.4}$$

If y is a root of $\xi^2 = \frac{b^2}{a^2-b^2D}$, let $x = -\frac{ay}{b}$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ Dy & x \end{pmatrix} = \begin{pmatrix} ax+byD & 0 \\ cx+dyD & cy+dx \end{pmatrix}.$$

If $b = 0$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}.$$

Therefore, every coset of N_D in $SL(2,\mathbb{F}_p)$ has a representative of the form $\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}$. If two such matrices $\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}$ and $\begin{pmatrix} x & 0 \\ y & x^{-1} \end{pmatrix}$ are in the same coset, then

$$\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}^{-1}\begin{pmatrix} x & 0 \\ y & x^{-1} \end{pmatrix} = \begin{pmatrix} xa^{-1} & 0 \\ ay-cx & ax^{-1} \end{pmatrix} \in N_D.$$

Thus we have

$$\left\{\begin{array}{rcl} xa^{-1} & = & ax^{-1}, \\ ay & = & cx, \end{array}\right. \tag{4.5}$$

or

$$\left\{\begin{array}{rcl} xa^{-1} & = & -ax^{-1}, \\ ay & = & cx, \end{array}\right. \tag{4.6}$$

Equation (4.6) gives $(xa^{-1})^2 = -1$, which is impossible since $p \equiv 3 \pmod 4$. From (4.5), we have

$$\left\{\begin{array}{rcl} a^2 & = & x^2, \\ ay & = & cx, \end{array}\right.$$

which implies

$$\left\{\begin{array}{l} a = x, \\ c = y, \end{array}\right. \text{ or } \left\{\begin{array}{l} a = -x, \\ c = -y. \end{array}\right.$$

Therefore R_D is a collection of coset representatives of N_D in $SL(2,\mathbb{F}_p)$.

(2)For $p \equiv 1 \pmod 4$, suppose that $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{F}_p)$. If $\xi^2 = \frac{b^2}{b^2D-a^2}$ is solvable over $\mathbb{F}_p$, then by (4.4), there exist a lower triangle matrix, such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and this lower triangle matrix are in the same coset.

Otherwise $\xi^2 = \frac{a^2}{a^2D-b^2D^2}$ is solvable over $\mathbb{F}_p$. let y be a root of $\xi^2 = \frac{b^2}{b^2D-a^2}$ and $x = \frac{byD}{a}$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ -Dy & -x \end{pmatrix} = \begin{pmatrix} 0 & ay-bx \\ cx-dyD & cy-dx \end{pmatrix}.$$

Therefore, every coset representative has the form $\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}$ or $\begin{pmatrix} 0 & x^{-1} \\ -x & y \end{pmatrix}$.

If two such matrices $\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}$ and $\begin{pmatrix} x & 0 \\ y & x^{-1} \end{pmatrix}$ are in the same coset, then equations (4.5) and (4.6) imply

$$\left\{\begin{array}{l} a = x, \\ c = y, \end{array}\right. \text{ or } \left\{\begin{array}{l} a = -x, \\ c = -y, \end{array}\right. \text{ or } \left\{\begin{array}{l} a = \sqrt{-1}x, \\ c = \sqrt{-1}y, \end{array}\right. \text{ or } \left\{\begin{array}{l} a = -\sqrt{-1}x, \\ c = -\sqrt{-1}y, \end{array}\right.$$

where $\sqrt{-1}$ is the smaller root of the equation $X^2+1=0$. Therefore

$$\left\{\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix} : a \in S, 0 \leq c \leq p-1\right\}$$

includes $\frac{p(p-1)}{4}$ different coset representatives of N_D in $SL(2,\mathbb{F}_p)$.

Similarly,

$$\left\{\begin{pmatrix} 0 & x^{-1} \\ -x & y \end{pmatrix} : x \in S, 0 \leq y \leq p-1\right\}$$

includes $\frac{p(p-1)}{4}$ coset different representative elements of N_D in $SL(2,\mathbb{F}_p)$.

If two such matrices $\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}$ and $\begin{pmatrix} 0 & x^{-1} \\ -x & y \end{pmatrix}$ are in the same coset, then

$$\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 0 & x^{-1} \\ -x & y \end{pmatrix} = \begin{pmatrix} 0 & a^{-1}x^{-1} \\ -ax & -cx^{-1}+ay \end{pmatrix} \in N_D.$$

Thus we have $a^{-1}x^{-1} = -Dax$ or $a^{-1}x^{-1} = Dax$, which implies $-D$ or D is a square element of $\mathbb{F}_p$. Both of them are impossible since $p \equiv 1 \pmod 4$.

Therefore,

$$\begin{aligned} R_D' &= \left\{\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & x^{-1} \\ -x & y \end{pmatrix} : a, x \in S, 0 \leq c, y \leq p-1\right\} \\ &= \left\{\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}, \begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : a \in S, 0 \leq c \leq p-1\right\} \end{aligned}$$

is a collection of coset representatives of N_D in $SL(2,\mathbb{F}_p)$. □

In the following, we give an algorithm for constructing the non-split finite oscillator dictionary $\mathfrak{S}^{ns}$.

Algorithm for $\mathfrak{S}^{ns}$

(1) For a given p, choose a non-square element D of $\mathbb{F}_p$, and s and t such that $s+t\sqrt{D}$ is a primitive element of $\mathbb{F}_{p^2}$.

(2) Let $g_D = \begin{pmatrix} \frac{s^2+Dt^2}{s^2-Dt^2} & \frac{-2st}{s^2-Dt^2} \\ \frac{-2stD}{s^2-Dt^2} & \frac{s^2+Dt^2}{s^2-Dt^2} \end{pmatrix}$. Diagonalize $\rho(g_D)$ to obtain $\mathcal{B}_T$.

(3) If $p \equiv 3 \pmod 4$, then

$$\mathfrak{S}^{ns} = \left\{S_a \circ N_{ac}(\varphi) : \ \varphi \in \mathcal{B}_T, 1 \leq a \leq \frac{p-1}{2}, 0 \leq c \leq p-1\right\}.$$

If $p \equiv 1 \pmod 4$, then

$$\mathfrak{S}^{ns} = \{S_a \circ N_{ac}(\varphi) : \ \varphi \in \mathcal{B}_T \cup F \circ \mathcal{B}_T, a \in S, 0 \leq c \leq p-1\}.$$

Remark 4.4. The above results can be easily generalized from $\mathbb{F}_p$ to $\mathbb{F}_{p^n}$.

References

1. D. Bump, *Automorphic Forms and Representations*, Cambridge University Press, Cambridge, 1998.
2. S.W. Golomb and G. Gong, *Signal Design with Good Correlation: for Wireless Communications, Cryptography and Radar Applications*, Cambridge University Press, Cambridge, 2005.
3. S. Gurevich, R. Hadani, and N. Sochen, The finite harmonic oscillator and its applications to sequences, Communication and radar, *IEEE Trans. Inform. Theory*, Vol 54, No.9, Sep. 2008, pp. 4239-4253.

4. S. Gurevich, R. Hadani, and N. Sochen, On some deterministic dictionaries supporting sparsity, *Journal of Fourier Analysis and Applications*, Vol. 14, No. 5-6, Dec. 2008, pp. 859-876.
5. S. Gurevich, R. Hadani, On the diagonalization of the discrete Fourier transform, *Applied and Computational Harmonic Analysis*, Vol. 27, Issue 1, July 2009, pp. 87-99.
6. S. Gurevich, R. Hadani, R. Howe, Quadratic reciprocity and sign of Gauss sum via the finite Weil representation, accpeted by *IMRN*. http://arxiv.org/abs/0808.2447.
7. S. Gurevich, R. Hadani, The statistical restricted isometry property and the Wigner semicircle distribution of incoherent dictionaries. Submitted to the *Annals of Applied Probability* 2009.
8. R. Howe, Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries, *Indag. Math.(N.S.)*, vol.16, no.3-4, 2005, pp. 553-583.
9. S. D. Howard, A.R. Calderbank, and W. Moran, The finite Heisenberg- Weyl groups in radar and communications, *EURASIP J. Appl. Signal Process.*, 2006:85685, 2006.
10. I. I. Piatetski-Shapiro, Complex representations of $GL(2, K)$ for finite fields K, Contemporary Math., 16, Amer. Math. Soc., providence, 1983.
11. A. Terras, *Fourier Analysis on Finite Groups and Its Applications*, London Mathematical Society Student Texts 43, Cambridge University Press, Cambridge, 1999.
12. Z. Wang, G. Gong, New sequences design from Weil representation with low two-dimensional correlation in both time and phase shifts, http://arxiv.org/abs/0812.4487, Technical Report 2009-1, University of Waterloo, 2009.
13. Z. Wang, G. Gong, A note on the diagonalization of the discrete Fourier transform, *Applied and Computational Harmonic Analysis*, Vol. 28, Issue 1, Jan. 2010, pp.114-120.
14. A. Weil, Sur certains groupes d'opéarateurs unitaires, *Acta Math.*, vol 111, 1964, pp. 143-211.
15. H. Weyl, *The Classical Groups. Their Invariants and Representations*, Princeton, N.J.: Princeton Univ. Press, 1939.

LMAM, School of Mathematical Sciences, Peking University, Beijing 100871, P.R. China

E-mail address: fengrq@math.pku.edu.cn

School of Mathematical Sciences, Suzhou University,Suzhou 215006, P.R. China

E-mail address: guzhmath@gmail.com

LMAM, School of Mathematical Sciences, Peking University, Beijing 100871, P.R. China

E-mail address: wzlmath@gmail.com

Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, P.R. China

E-mail address: whfmath@gmail.com

Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, P.R. China

E-mail address: kzhou@amss.ac.cn